# Improving Ideal Arithmetic

Michael J. Jacobson, Jr.

jacobs@cpsc.ucalgary.ca

UNIVERSITY OF CALGARY

UNCG Summer School in Computational Number Theory 2016: Function Fields

# Applications of Ideal Arithmetic

Arithmetic of ideal of function fields has many applications:

- invariant computation (class group, regulator / fundamental units)
- cryptography
- constructing cubic function fields of a given discriminant

For all, want the arithmetic to be as fast as possible. Minimize:

- number of field multiplications
- number of inversions (about 100 muls each in odd char, 10 in even)

# Approaches to Speed Ideal Arithmetic

Optimization for arithmetic can happen at three levels:

- Optimize arithmetic in the field $K$
- Optimize divisor class arithmetic
- Optimize certain arithmetic operations in the class group (e.g. tripling, scalar multiplication)

Approaches to fast divisor class arithmetic:

- Optimize addition/reduction formulas
  - Optimize generic formulas (e.g. NUCOMP)
  - Optimize for fixed, small genus (explicit formulas)
- Use different curve/function field descriptions

# Divisor Addition

Recall the formulas for divisor addition:

## Theorem

*Let* $D_1 = (u_1, v_1)$ *and* $D_2 = (u_2, v_2)$ *be semi-reduced divisors. Then* $D_1 + D_2 = D + \mathrm{div}(s)$ *where* $D = (u, v)$ *is a semi-reduced divisor, and* $s, u, v \in \mathbb{F}_q[x]$ *are computed as follows:*

1. *Let* $s = \gcd(u_1, u_2, v_1 + v_2 + h) = au_1 + bu_2 + c(v_1 + v_2 - h)$
2. *Set* $u = \dfrac{u_1 u_2}{s^2}$.
3. *Set* $v = \dfrac{au_1 v_2 + bu_2 v_1 + c(v_1 v_2 + f)}{s} \pmod{u}$

# NUCOMP

Problem with add/reduce:

- Mumford representation of reduced ideal/divisor has $\deg(u) \leq g$
- intermediate operands (before reduction) have degree $\leq 2g$

NUCOMP (Shanks 1988):

- apply partial reduction *before* multipliction, to reduce operand sizes
- Shanks: composition of positive-definite binary quadratic forms
- J./van der Poorten (2002), J./Scheidler/Stein (2007): generalized to hyperelliptic function fields
- more complicated algorithm, but intermediate operands usually have degree $\leq 3g/2$
- J./Scheidler/Stein (2007): faster for $g > 6$ (roughly)

# NUCOMP: Main Idea

Consider $(u_1, v_1) + (u_2, v_2) = (u, v)$. Set $w_2 = (f + hv_2 - v_2^2)/u_2$.

- From addition law:

$$v \equiv \frac{au_1v_2 + bu_2v_1 + c(v_1v_2 + f)}{s} \pmod{u}$$
$$= v_2 + U\frac{u_2}{s} \text{ with } U \equiv b(v_1 - v_2) + cw_2 \pmod{u_1/s}$$

- reduction of $(u, v) \leftrightarrow$ continued fraction expansion of $(v + y)/u$
- rational function $sU/u_1 \approx (v + y)/u$ (irrational)
- rational continued fraction expansion gives same partial quotients as the irrational one (first few iterations)
- can derive formulas to compute reduction of $(u, v)$ without first computing $u$ and $v$

# NUCOMP: Description ($C : y^2 = f(x)$)

1. Compute $s, U$ as before. Set $L = u_1/s$, $N = u_2/s$.
2. Set $R_{-2} = U$, $R_{-1} = u_1/s$, $C_{-2} = -1$, $C_{-1} = 0$. Iterate

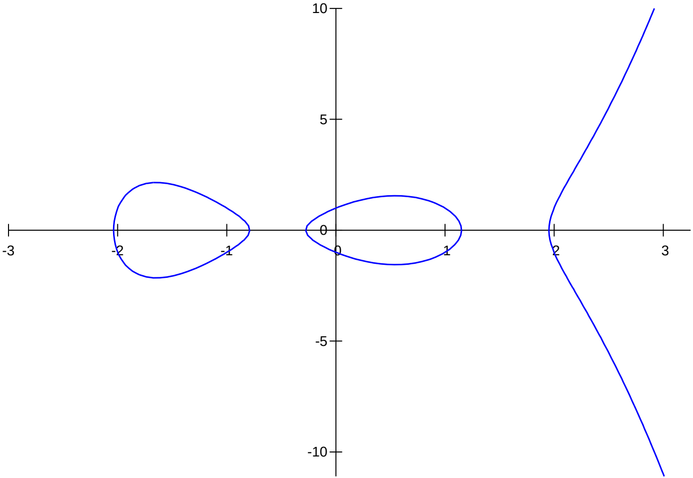
$$q_i = \lfloor R_{i-2}/R_{i-i} \rfloor, \quad R_i = R_{i-2} - q_i R_{i-1}, \quad C_i = C_{i-2} - q_i C_{i-1}$$

until $\deg(R_i) \leq (\deg(u_1) - \deg(u_2) + g + (g \bmod 2))/2 < \deg(R_{i-1})$

3. Compute:
   - $M_1 = (NR_i - (v_1 - v_2)C_i)/L$
   - $M_2 = (R_i(v_1 + v_2) - sw_2 C_i)/L$
   - $u = (-1)^{i-1}(R_i M_1 - C_1 M_2)$
   - $v = (NR_i + uC_{i-1})/C_i - v_2 \pmod{u}$

# Geometric Method: An Example

$H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$



# The Jacobian (geometrically)

**Jacobian** of $H$: $\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}^0_H(\overline{K})/\mathrm{Prin}_H(\overline{K})$

Motto: "*Any complete collection of points on a function sums to zero.*"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

For elliptic curves: $E(\overline{K}) \cong \mathrm{Jac}_E(\overline{K}) \quad (\Rightarrow \ E(\overline{K})$ is a group)

**Identity:** $[\infty] = \infty - \infty$

**Inverses**: The points

$$P = (x_0, y_0) \ \text{ and } \ \overline{P} = (x_0, -y_0 - h(x_0))$$

on $H$ both lie on the function $x = x_0$, so

$$-[P] = [\overline{P}]$$

# Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of $P$, $\overline{P}$ can appear (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**. If $\sum m_P \leq g$, then it is **reduced**.

E.g. $g = 2$: reduced divisors are of the form $[P]$ or $[P] + [Q]$.

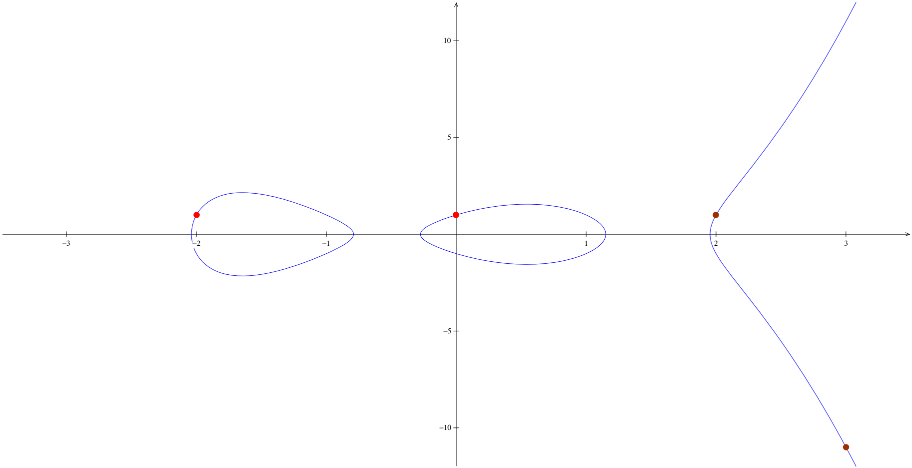
**Theorem**

*Every class in $\mathrm{Jac}_H(\overline{K})$ contains a unique reduced divisor.*

$D_1 \oplus D_2$: the reduced divisor in the class $[D_1 + D_2]$

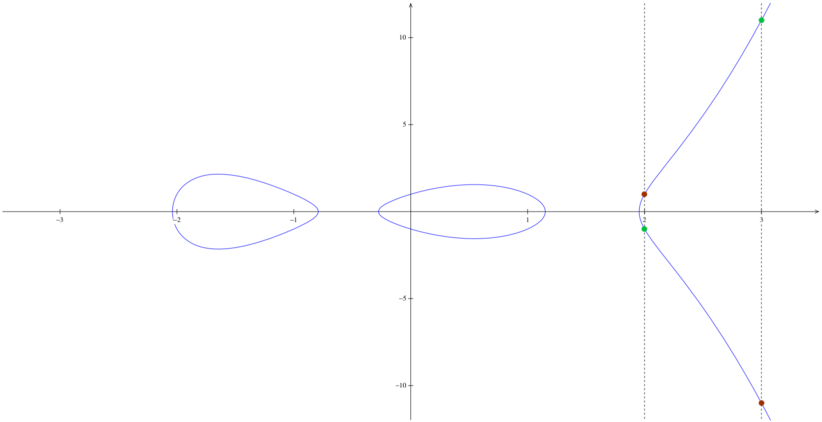
# An Example of Reduced Divisors

$D_1 = (-2, 1) + (0, 1)$ , $D_2 = (2, 1) + (3, -11)$



# Inverses on Hyperelliptic Curves

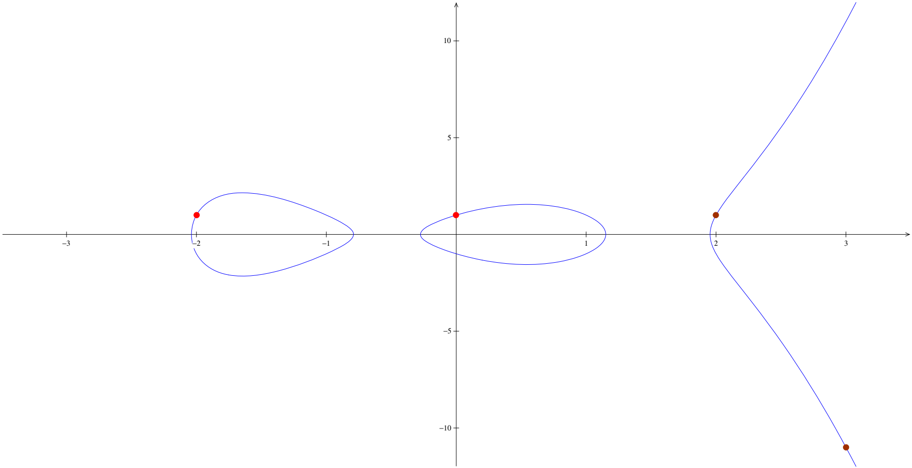
The inverse of $D = P_1 + P_2 + \cdots P_r$ is $-D = \overline{P}_1 + \overline{P}_2 + \cdots \overline{P}_r$



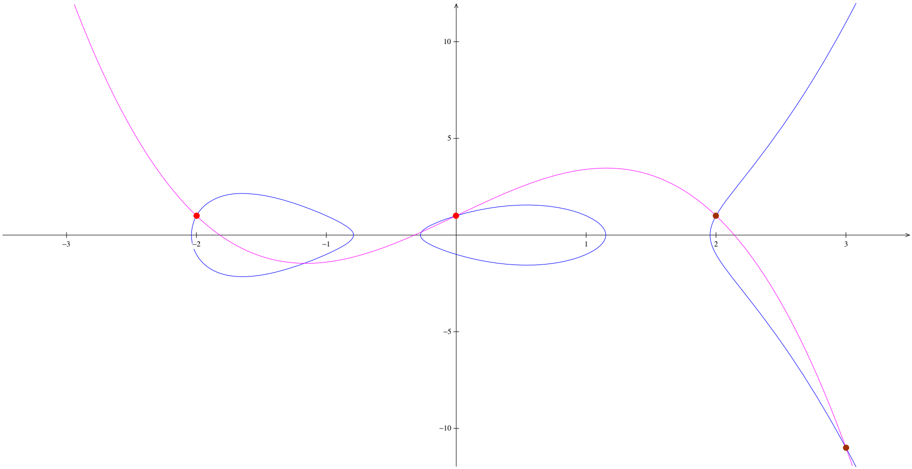

$$-(\bullet + \bullet) = (\bullet + \bullet)$$

# Addition on Genus 2 Curves

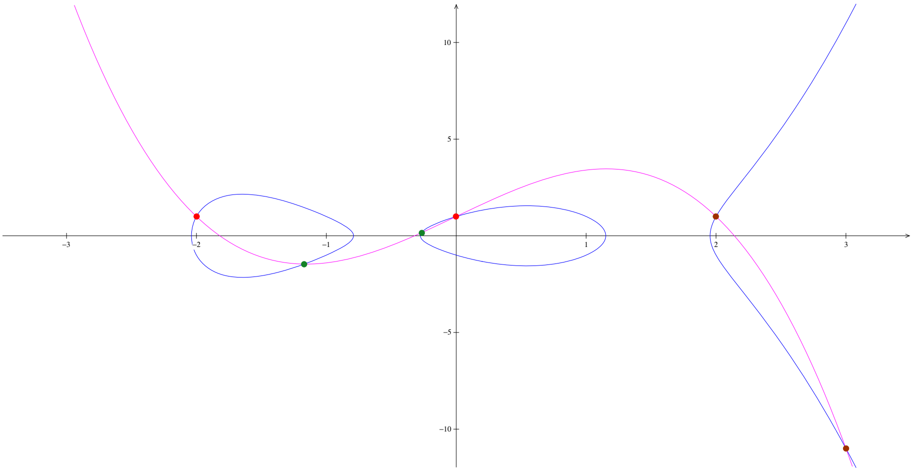
$D_1 = (-2,1) + (0,1)$ , $D_2 = (2,1) + (3,-11)$



# Addition on Genus 2 Curves

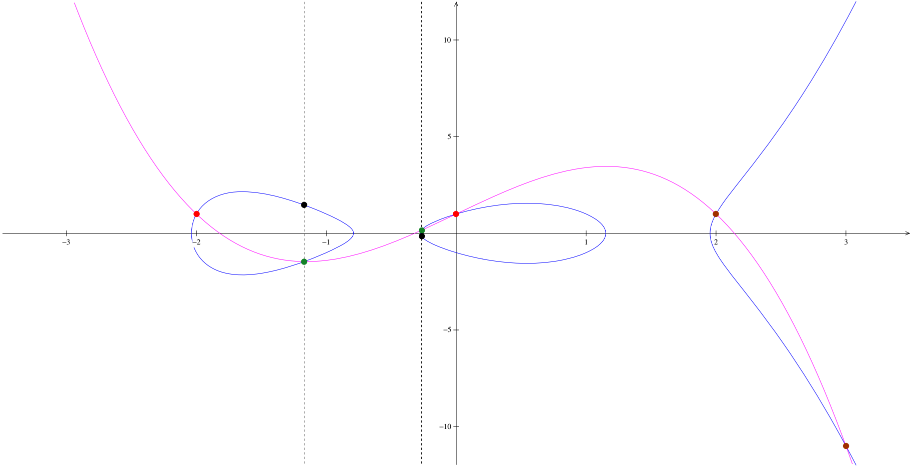


# Addition on Genus 2 Curves




$$(\bullet + \bullet) + (\bullet + \bullet) + (\bullet + \bullet) = 0$$

# Addition on Genus 2 Curves




$$(\textcolor{red}{\bullet} + \textcolor{red}{\bullet}) + (\textcolor{orange}{\bullet} + \textcolor{orange}{\bullet}) + (\textcolor{green}{\bullet} + \textcolor{green}{\bullet}) = 0 \quad \Rightarrow \quad (\textcolor{red}{\bullet} + \textcolor{red}{\bullet}) \oplus (\textcolor{orange}{\bullet} + \textcolor{orange}{\bullet}) = (\bullet + \bullet)$$

# Addition on Genus 2 Curves

Motto: "*Any complete collection of points on a function sums to zero.*"

To add and reduce two divisors $P_1 + P_2$ and $Q_1 + Q_2$ in genus 2:

- The four points $P_1$, $P_2$, $Q_1$, $Q_2$ lie on a unique function $y = v(x)$ with $\deg(v) = 3$.
- This function intersects $H$ in two more points $R_1$ and $R_2$:
  - The $x$-coordinates of $R_1$ and $R_2$ can be obtained by finding the remaining two roots of $v(x)^2 + h(x)v(x) = f(x)$.
  - The $y$-coordinates of $R_1$ and $R_2$ can be obtained by substituting the $x$-coordinates into $y = v(x)$.
- Since $(P_1 + P_2) + (Q_1 + Q_2) + (R_1 + R_2) = 0$, we have

$$(P_1 + P_2) \oplus (Q_1 + Q_2) = \overline{R_1} + \overline{R_2} .$$

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r - 2, 2g + 1\}$.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r - 2, 2g + 1\}$.
  $r$ of the roots of $w(x)$ are the $x$-coordinates of the $P_i$.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r-2, 2g+1\}$. $r$ of the roots of $w(x)$ are the $x$-coordinates of the $P_i$.
- If $r \geq g + 2$, then $\deg(w) = 2r - 2$, yielding $r - 2$ further roots.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r-2, 2g+1\}$.
  $r$ of the roots of $w(x)$ are the $x$-coordinates of the $P_i$.
- If $r \geq g+2$, then $\deg(w) = 2r - 2$, yielding $r - 2$ further roots.
  If $r = g+1$, then $\deg(w) = 2g+1$, yielding $g$ further roots.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r - 2, 2g + 1\}$. $r$ of the roots of $w(x)$ are the $x$-coordinates of the $P_i$.
- If $r \geq g + 2$, then $\deg(w) = 2r - 2$, yielding $r - 2$ further roots. If $r = g + 1$, then $\deg(w) = 2g + 1$, yielding $g$ further roots.
- Substitute these new roots into $y = v(x)$ to obtain $\max\{r - 2, g\}$ new points on $H$.

# Geometric Reduction

To reduce $D = \sum_{i=1}^{r} [P_i]$, iterate as follows until $r \leq g$:

- The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r - 2, 2g + 1\}$. $r$ of the roots of $w(x)$ are the $x$-coordinates of the $P_i$.
- If $r \geq g + 2$, then $\deg(w) = 2r - 2$, yielding $r - 2$ further roots. If $r = g + 1$, then $\deg(w) = 2g + 1$, yielding $g$ further roots.
- Substitute these new roots into $y = v(x)$ to obtain $\max\{r - 2, g\}$ new points on $H$. Replace $D$ by the new divisor thus obtained.

Since $r \leq 2g$ at the start, $D_1 \oplus D_2$ is obtained after at most $\lceil g/2 \rceil$ steps.

# Addition in Genus 2 – Example

Consider $H : y^2 = f(x)$ with $f(x) = x^5 - 5x^3 + 4x + 1$ over $\mathbb{Q}$.

To add & reduce $(-2, 1) + (0, 1)$ and $(2, 1) + (3, -11)$, proceed as follows:

- The unique degree 3 function through $(-2, 1)$, $(0, 1)$, $(2, 1)$ and $(3, -11)$ is $y = v(x)$ with $v(x) = -(4/5)x^3 + (16/5)x + 1$.
- The equation $v(x)^2 = f(x)$ becomes
$$(x - (-2))(x - 0)(x - 2)(x - 3)(16x^2 + 23x + 5) = 0 \ .$$
- The roots of $16x^2 + 23x + 5$ are $\dfrac{-23 \pm \sqrt{209}}{32}$.
- The corresponding $y$-coordinates are $\dfrac{-1333 \pm 115\sqrt{209}}{2048}$. So
$(-2, 1) + (0, 1) \ \oplus \ (2, 1) + (3, -11) =$
$$\left(\frac{-23 + \sqrt{209}}{32}, \frac{1333 - 115\sqrt{209}}{2048}\right) + \left(\frac{-23 - \sqrt{209}}{32}, \frac{1333 + 115\sqrt{209}}{2048}\right).$$

# Geometric Method with Mumford Representations

**Problem:** divisors are usually represented with polynomial pairs (Mumford) as opposed to formal sums of points

Costello/Lauter (2011): problem solved!

- find interpolating polynomial $\ell(x)$ via linear system solving
  - $\ell(x) - v_i(x) \equiv 0 \pmod{u_i(x)}$ yields $g$ linear equations in the coefficients of $\ell$
  - combining equations from $(u_1, v_1)$ and $(u_2, v_2)$ yields a linear system of dimension $2g$
- avoid computing roots to find $u(x)$ :
  - compute $u(x)$ by equating coefficients of $u(x)u_1(x)u_2(x) = \ell(X)^2 - f(x)$
- compute $v(x) = \ell(x) \bmod u(x)$

# Explicit Formulas

Algorithms above are decribed in terms of polynomial arithmetic in $K[x]$.

- For fixed, small $g$, can express the operations in terms of arithmetic of field elements.
- Gives further opportunities to optimize (reduce field inverstions) and eliminate redundant computations

Some techniques used:

- Compute resultant instead of GCD (via Bezout's matrix)
- Optimize exact polynomial divisions
- "Montgomery's Trick" for simultaneous inversions: compute $I = (xy)^{-1}$, $x^{-1} = Iy$, $y^{-1} = Ix$
- Karatsuba for polynomial multiplication, polynomial reduction

# Inversion-Free Arithmetic via Projectivization

Represent the divisor

$$(u, v) \text{ with } u = x^2 + u_1 x + u_0 \text{ and } v = v_1 x + v_0$$

with

$$[u_1', u_0', v_1', v_0', z] \text{ where } u_1 = u_1'/z,\ \ u_0 = u_0'/z,\ \text{ etc.}$$

Idea:

- extra coordinate $z$ accumulates values that would have been inverted
- multiply representation through by $z$ to clear denominators and avoid inversions

Fastest formulas for genus 2, odd characteristic:

- Hisil/Costello (2014): Jacobian coordinates (weighted projectivization requiring three extra coefficients)

# Explicit Formulas: state-of-the-art

Genus 2 hyperelliptic curves (ramified model):

- Lange et al.: very well developed (explicit versions of algebraic method)
- Costello/Lauter (2011): explicit formulas for genus 2 using geometric method
- Lindner/Imbert/J. (2016): combination of algebraic and geometric, double-add, triple

Higher genus (ramified models):

- Very well developed for genus 3
- Pelzl et al. 2003: explicit formulas for genus 4 ramified models
- Research in progress for split models